GOTBOTS?

HOW TO EVALUATE SOLUTIONS FOR BOT MANAGEMENT & MITIGATION

Akamai

GOTBOTS?

HOW TO EVALUATE SOLUTIONS FOR BOT MANAGEMENT & MITIGATION

CHAPTER 1 // GOOD BOT. BAD BOT. WHAT'S THE REAL DIFFERENCE?

- How to classify each type of bot and what they do.
- Why you should keep an open mind about allowing bot activity.
- Why the bot is just an automated tool – it's the bot operator.

CHAPTER 2 // THE CHALLENGE OF BOT MITIGATION

- Why bot mitigation or blocking falls short and how it can adversely affect your business.
- Why a single technique for bot detection is not sufficient in today's Internet landscape.
- Why you need a deeper level of bot detection and visibility as well as control over all bot activity.

CHAPTER 3 // PARADIGM: STEPS TO SUCCESSFUL BOT MANAGEMENT

- How a new paradigm of bot management helps e-commerce and online businesses make more informed decisions on how to handle bot activity.
- What best practices IT can use to identify, quantify, and manage bot traffic.
- How IT can tap into a wide range of bot management strategies to manage bot traffic without alerting the operator.

CHAPTER 4 // EVALUATING BOT MANAGEMENT SOLUTIONS

- What key capabilities should be part of a comprehensive bot management solution.
- How a bot management solution can complement other web security measures for detecting cyberattacks and other threats.

CHAPTER 5 // ADOPTING A PROACTIVE BOT MANAGEMENT PROCESS

- How a proactive, long-term approach to bot management can reduce the impact of bot activity on the web application infrastructure and business as a whole.
- What actions IT can take through a bot management solution to better control bot activity.
- How a proactive approach to bot management can help online businesses be more competitive.

BOTS ARE A FACT OF LIFE

If "block" is the first word that comes to your mind when your IT staff reports bot activity on your website, you're not alone. However, contrary to popular belief, bots are not always bad. A bot, or Internet robot, is simply a piece of software running on a server connected to the Internet. As with any piece of software, a variety of different bot operators – ranging from individuals to criminal organizations to legitimate businesses – create bots to perform a variety of different tasks. With the advantage of automation, operators typically employ bots to perform tasks that are highly repetitive in nature. Much of what transpires on the web every day is, in fact, performed by bots, from search-engine indexing to website monitoring and DDoS attacks.

Bots are a fact of life for any organization doing business online. For many companies, an estimated 40% of online traffic is generated by bots. The fact is that bots will never go away, because there is information online that people and businesses need, and it is easier and faster to get that information in an automated fashion. In fact, if you do business online you should have a strategic plan in place to get the most out of the good bots that are coming to your site representing customers, partners, and third-party information providers such as search engines.

Bots become problematic when they are employed by malicious actors, and it's clear that blocking these bots doesn't work. In fact, blocking triggers the bot to mutate, and therein lies the challenge. Bots are here to stay, so they should be approached more as a permanent challenge rather than an occasional problem to be solved. The bottom line: refrain from blocking bots as much as possible and instead consider alternate behavior for a more efficient bot management strategy. It makes the most sense to manage bots much as you do the activities of all other users of your website and web applications. Do bots hinder or help you have a strong online presence? When you can answer that question, you can develop strategies to best manage the impact of either than hindrance or helpfulness.

In this e-book, you'll learn that as bots become more sophisticated, a single method of managing bots – that is to say, blocking – simply cannot cover all of the different types of bots that are interacting with your web applications. What's more, bot operators can evolve their bots over time, so while their first attempt may be successfully blocked, they can counter with a stealthier approach that is not as easily detected. That is why, instead of the traditional approach to blocking as the key strategy for bot mitigation, today's bot landscape requires a shift to proactive bot management. An approach with improved bot detection and advanced bot responses at the core is the new recommended best practice for web-based businesses.

Read on to learn more.

CHAPTER // 1

GOOD BOT. BAD BOT. WHAT'S THE REAL DIFFERENCE

If bots are not necessarily bad, when are they bad? And when are they good? Because many different operators create bots to perform many different tasks, it's impossible to generalize the impact that bots can have. Realistically, some bots — like search-engine crawlers or social media and online advertising bots — are good, and some bots – such as those designed to launch DDoS attacks – are bad, but most bots will fall somewhere in between. However, keep in mind that what may be good or bad for one organization may not be for another. The definition of what constitutes a good or bad bot clearly lies in the eye of the beholder and is based on the impact the bot has on business and website performance.

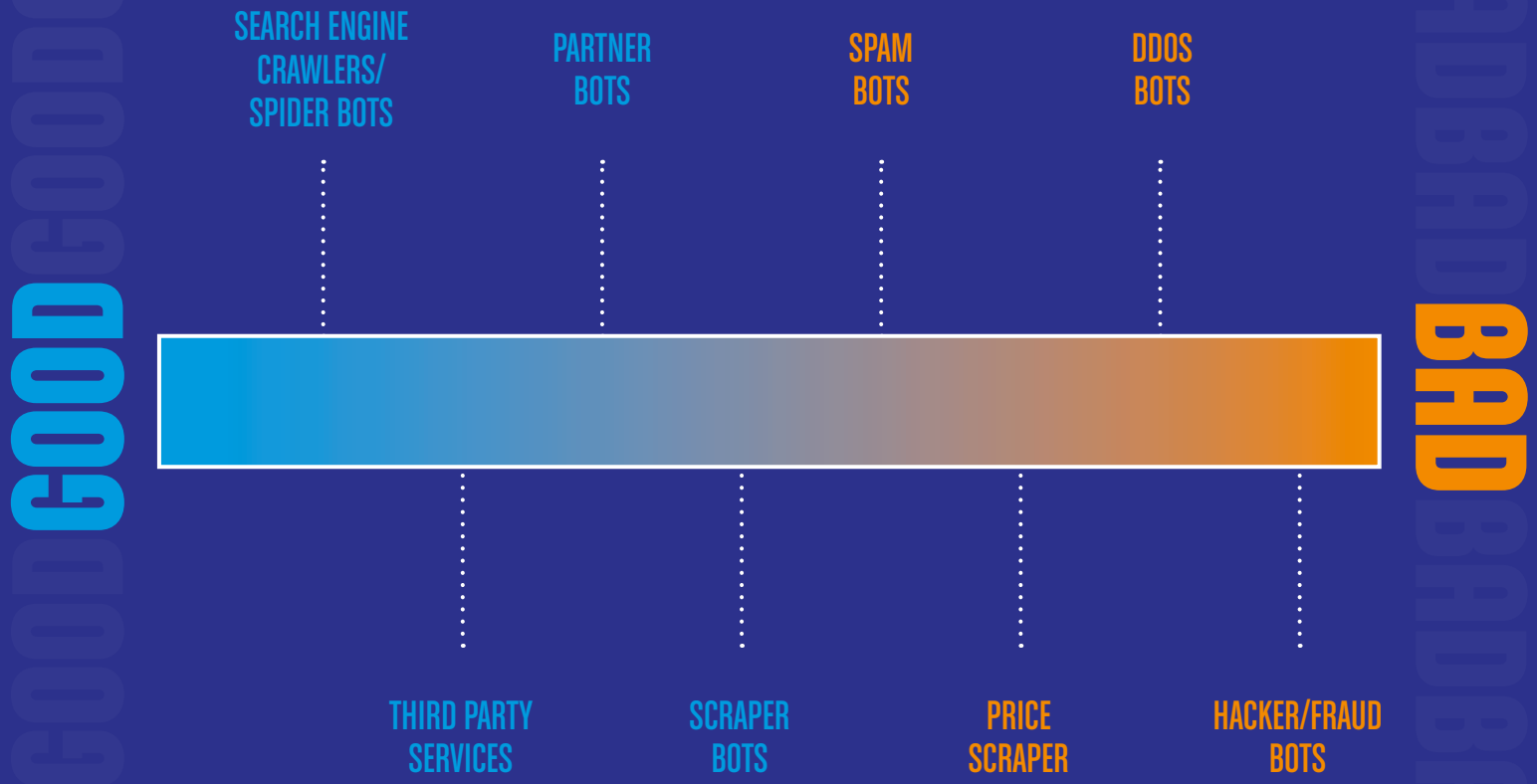
What organizations need is a framework to better understand the nature of bots and the impact that they have on their business. This framework starts with the website – how does it fit into the organization's online strategy. How is it intended to be used? If you can answer this question, then you can identify behavior that either falls within the guidelines of intended use (good) or misuse (bad). Next, you need to consider the bot itself. How is it interacting with the website? Who created it? What is the intent or purpose? There are many situations in which the same bot can exhibit behavior that can be both good and bad, depending on who created the bot and why.

In addition, how a bot behaves may cause a disconnect between the advantage to the business and the impact on IT. A good example is Baidu. Allowing this search engine on your site can have a positive business impact, especially if you want to do business in China. However, Baidu is well known as a very aggressive bot that can cause a high load on the origin. The bot's behavior degrades the web experience for other users, which becomes a negative business impact. As a result, companies must decide if they want to make a tradeoff between theoretical positive business impact and a known negative IT impact. Some companies actually block Baidu because of the performance impact and lose the advantage of online visibility within the China marketplace. That is why a clear understanding of bot use cases is so important.

UNDERSTAND THE USE CASE

When we look at the different ways that bots interact with websites, a number of use cases, or groups of bots with similar purpose and behavior, become readily apparent. As the graphic on the next page illustrates, the purpose and behavior of a bot can be good or bad, ranging from a search engine bot indexing a site to bots being used by hackers and DDoS attackers with malicious.

E-commerce companies need to gain an understanding of the many types of bots and how each one can affect business and IT infrastructure.


GOOD
BAD
SEARCH ENGINE CRAWLERS/ SPIDER BOTS
PARTNER BOTS
SPAM BOTS
DDOS BOTS
THIRD PARTY SERVICES
SCRAPER BOTS
PRICE SCRAPER
HACKER/FRAUD BOTS

SEARCH ENGINE CRAWLERS/SPIDER BOTS

Google, Yahoo, Infoseek, and other less well-known search engines deploy bots to gather information for indexing millions of websites. These are beneficial to the business because they use data based on page titles, keywords, text, and more to determine ranking when users browse and search for specific information on products, services, and more. Most search engines also use spider bots that "crawl" from one hyperlink to another. Spiders enable search engines to keep track of how many links to external pages are active, a factor upon which search engines rank search-engine results.

THIRD-PARTY SERVICES

Organizations often contract with third-party services that employ bots to perform search engine optimization (SEO), or test the performance and security of their web-facing network. The impact on the network can vary – IT can usually specify the amount of resources the bot can use. However, third-party services are often contracted by other groups within the organization who may not inform IT and may not be considering the performance impact

PARTNER BOTS

E-commerce businesses and many other types of online organizations may allow business partners such as resellers and third-party service providers to use bots to scrape current product and pricing information from their websites, or any other type of information that is valuable to sales and marketing efforts.

CONTENT AGGREGATION AND SCRAPINGS

Scrapers are automated tools that attempt to steal digital assets, many times in order to increase the traffic to the thief's website without credit to the original content owner. This is particularly a problem for media sites, since their intellectual property is ingrained in their content. These bots mine various types of publicly available news and media content from websites with the purpose of publishing the information on multiple third-party websites. The purpose is to drive user traffic away from the original owner of the content to the third-party website.

FORM/COMMENT SPAM

Bots with the ability to insert records into databases can skew real-user statistics. This is particularly important as companies try to monetize analytics through big data. Spammers also affect the brand perception whenever a legitimate website is defaced with comments about drugs, sexuality, and other controversial issues. Spammers often add links in their comments than can drive traffic to unauthorized sites and affect SEO behavior.

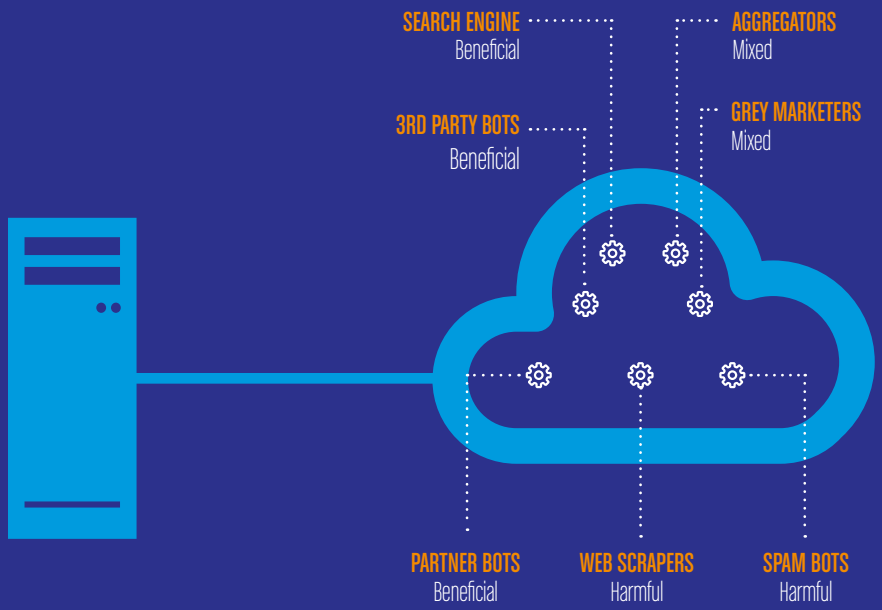
INVENTORY GRABBERS/GRAY MARKETERS

Inventory grabbers use automated bot software to quickly reserve new products in shopping carts as soon as they are available. Gray marketers try to upsell their purchases in other markets like eBay. Large global sporting goods, retail, and electronics companies have encountered these problems. Inventory grabbing is also an issue for airlines or event ticketing companies when bots snap up desirable seats and then release only the less desirable ones – often with little time left to sell.

PRICE SCRAPING

Bot operators from competitive businesses can scrape pricing from e-commerce sites for competitive intelligence purposes, – for example, to gain an edge by offering a lower price than the competitor. Of course, price-scraping activity can also originate from legitimate price comparison websites, so these bots are not always detrimental to the business.

Not all bots are bad, but they all increase the load on your infrastructure



IT'S NOT THE BOT. IT'S THE BOT OPERATOR.

So far, we've talked about the disparate use cases for different types of bots. But these computers are not HAL from 2001: A Space Odyssey – they are being programmed by someone with specific intentions. Behind every bot is an operator – a human individual or someone working for a business that has created the automated robot for the specific purpose of getting information or performing an action on a website. If IT blocks the bot, the operator will know, and the bot operator will simply update the bot signature to try again. Many bot operators are financially motivated to get the information, so every time they detect a block they will continue to return more stealthily than before, making it difficult — if not impossible — to detect them.

A strong bot management strategy, therefore, starts by thinking through the bot operator's intention first, based on the impact you are seeing on your business and your web infrastructure.

THE IMPACT ON THE BUSINESS AND IT

The key point to understand is that bot activity can have a very different impact on business and IT respectively. It all depends on how the bot behaves on the site, even when the bot is performing a legitimate business service. If IT wants to block all bots to avoid degrading site performance or malicious activity, the business misses out on the benefits of legitimate bots that drive traffic to the site or provide critical information to business partners. That is why the IT team must be able to easily detect and analyze the intent of all of the various bots entering the network – and more importantly, be able to control how much traffic can be generated by a bot at any given time, instead of automatically blocking all bots.

For example, e-commerce sites may want to give preferential treatment to legitimate search engines like Google, business partners, and third-party bots that generate analytics for search-engine optimization. So it is in the best interest of the business that IT does not inadvertently block these bots or slow down the ability for them to retrieve information. But this is where bot management can get complicated. It is a business advantage to give resellers the ability to use web scrapers to obtain current product information, but IT would be remiss to allow the resellers' bots to bombard the site with extra traffic and slow down site performance for users at peak shopping times. In addition, the business can gain valuable information on website uptime or search-engine optimization performance through the analytics gathered by third-party bots. However, IT still must be able to easily identify third-party bots as "good" and be able to control how much bandwidth the bots can consume, so as to not allow them to affect site performance.

As you can see, bot management must take the entire enterprise into consideration, the challenges to the right illustrate:

CUSTOMER WEB EXPERIENCE

Customer relationship strategies rely on the business being able to respond quickly and consistently to customer needs. In an online business, website performance impacts the web experience, which drives customer engagement and sales transaction rates for the better or worse, depending on the performance quality. A site that's overloaded with bots may suffer in terms of performance, reducing customer engagement and sales.

DISTORTED USER ANALYTICS

Marketing departments use analytics tools to understand how sales relate to track how users are interacting with the website, but when there is a heavy amount of bot traffic coming in, it becomes more difficult to get an accurate picture of how the site is really being used by customers and other visitors. As a result of bot activity polluting the data, marketing gets a distorted view of activity on the site and inaccurate information on which to base future business decisions.

DAMAGED BRAND RECOGNITION AND LOYALTY

Third parties can use bots to prevent companies from enhancing customer relationships and building brand recognition. A typical example involves a global sports clothing company that creates a limited edition sneaker in a quantity of 10,000 as a special offer to their most avid customers. However, an inventory grabber bot infiltrates the website and buys up a large percentage of the shoes with the purpose of reselling them. When legitimate customers log on to the original sports site literally seconds after receiving the offer, they are disappointed and frustrated because the shoes have already sold out. The sports company has missed its opportunity to increase brand recognition, create a marketing buzz, and boost brand loyalty – all because of a bot.

LOST SALES AND MARKET SHARE

Content aggregation – the theft of the organization's thought leadership – is yet another example of how bots used for malicious purposes can damage brand recognition and loyalty – but also cause a loss of sales and market share. A company's thought leadership, in the form of industry information or proprietary research, is a sales tool that can be hijacked by bot activity. In this example, content theft or aggregation is particularly damaging to online businesses when the stolen content is published and promoted on one or multiple third-party websites. Customers and potential users of the original site seeking the information are now being driven to the third party rather than the content's originator. As a result, the owner of the stolen content suffers in terms of lost sales and upselling opportunities, loss of brand awareness, and reduced ability to build new market share.

LOST CUSTOMERS AND REDUCED COMPETITIVE ADVANTAGE

A competitive pricing strategy is critical to business profitability and customer satisfaction. Online shoppers are particularly price conscious, and they shop around with a few quick mouse clicks to find a better deal. Price scraping with intent to immediately undercut a competitor's pricing is a huge problem for all types of businesses that sell products and services online, regardless of industry or market. The e-commerce victims of price scraping lose sales, lose customers, and suffer damage to their competitive advantage.

ORIGIN LOAD AND PERFORMANCE IMPACT

All bots and their operators, whether with good or bad intentions, can put a load on the origin of a web infrastructure. Automated bots can create traffic spikes that can lead to site performance issues for legitimate users. If these anomalies caused by bots remain undetected or not analyzed, some companies choose to build out a web infrastructure larger than what they need and end up unnecessarily increasing infrastructure and origin costs. They may also increase operational costs by adding dedicated human and technical resources to analyze site traffic and block bots. Most companies, however, do not have these resources, and even if they did, the process of detecting and analyzing bot traffic is incredibly complex, since bot signatures constantly change over time.

STEP BACK AND GET THE WHOLE PICTURE

Bot management affects not only IT but also other departments across the enterprise – sales, marketing, customer service – that rely on website performance and accurate site analytics to ensure a satisfying user experience. Any bot activity that slows down or blocks users from purchasing goods or services, steals a company's thought leadership information, or prevents marketing from gathering accurate data to make competitive business decisions, is a much bigger problem than a churning website.

Therefore, there is a critical need for an expert bot management strategy that can solve problems that impact the business as a whole, not just IT infrastructure performance. This strategy must be a new paradigm that goes beyond typical bot mitigation. The next chapters in the e-book will explore how bot blocking can actually adversely affect your business and why adopting a proactive, long-term approach to bot management is the better, more competitive choice.

So, which bots should be blocked and which should not? The answer may surprise you. Read on to find out why blocking all bots is not the best solution.

CHAPTER // 2

THE CHALLENGE OF BOT MITIGATION

Solving the bot problem is not simply a matter of setting up a firewall or other security solution to block all bots. In fact, bots are really not a security problem at all. However, IT is still challenged to detect, identify, and analyze the wide range of bot activities, each of which can have varying impacts on business and IT infrastructure. They need answers to the questions: What is the bot doing? Why is it here? Who created it? What incentives are motivating the bot operator to keep coming back?

The lack of visibility and ability to identify the bot's purpose, in particular, is an issue that has compelled IT to take a reactive approach when alerted to an application performance or site availability issue caused by a bot. In their defense, when using traditional technologies, they are simply not equipped with the right detection, analysis, or control tools to make proactive decisions around bot management. The old-school thinking of "all bots are bad and must be blocked" is really the only strategy they have.

As the volume of non-human bot traffic to websites increases, organizations are exhausting more resources serving content to automated clients whose intent may be difficult to identify and whose behavior disrupts not only website performance, but also business strategies. In order to truly control the impact of bots on the business, IT must transition from a mindset of bot mitigation to bot management.

WHY CURRENT BOT MITIGATION PRACTICES FALL SHORT

Everyone in today's online commerce marketplace – from IT to third-party vendors and marketing departments – tends to think in black and white when categorizing bots into either good or bad, but in fact the impact that a bot can have on an organization is usually a gray area depending on the type of bot activity and type of business. Obviously, there is no question that a bot designed and launched to aggressively scan applications with the intent to steal user confidential data, such as credit card numbers and Social Security numbers, is bad for the business. Yet good bot traffic from a business partner bot, for example, can sometimes behave like a bad bot in some situations, such as performing aggressive scraping activity at critical shopping times of the month or year, such as on Black Friday. In a case like this, the partner bot not only impacts site performance and the user experience, but also impacts the ability of the business to generate a higher volume of sales and provide excellent customer service.

Nevertheless, many IT departments still treat bots as a security issue. Most bot mitigation solutions in the market today can do little beyond outright blocking and fall short because they do not provide IT groups with the required levels of detection, visibility, or control. In addition, current mitigation techniques overlook the fact that behind every bot is an operator – a human individual or someone working for a business — who has created the automated robot for the specific purpose of getting information or performing an action on an e-commerce website. If IT blocks the bot, the operator will know and will simply update the bot signature to try again. Bot operators are usually financially motivated to get the information, so every time they detect a block they will continue to return more stealthily than before, making it increasingly difficult — if not impossible — to detect them.

Clearly, blocking all bots is not the answer. Managing bots within a framework that allows organizations to apply different management actions to different types of bots based on their business and IT impacts – without alerting the bot operator – is smarter than mitigation.

CHAPTER // 3

A PARADIGM: STEPS TO SUCCESFUL BOT MANAGEMENT

Clearly, traditional IP blocking provides only temporary pain relief until the bot operator detects the block, changes the IP, and starts a new bot invasion. The good news is that a new paradigm of bot management is emerging that empowers IT to finally take a proactive approach to detecting, analyzing, and making informed decisions on how to handle all types of bot activity on their websites. Using this new approach, IT groups will be able to:

- *Identify known and unknown bots.*
- *Categorize bots based on business impact and detection method*
- *Assign appropriate management policies to every bot category*
- *Use a range of sophisticated methods to manage specific types of bot traffic.*
- *Minimize the burden on the origin server and minimize both business and IT impact.*

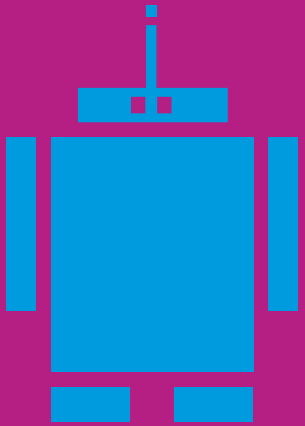
The concept of bot management is to give IT full control over how different types of bot traffic are handled in regard to the potential effect of the traffic on both the IT infrastructure and the organization's business. A best practice is to first categorize bots according to well-known and well-publicized bots that commonly interact with online businesses, individual bots specific to the company – both good and malicious – that IT may already know about, and unknown bots. This gives online businesses the flexibility to create specific policies to manage the activities of bots within each category according to how they impact both the business and the performance of the web infrastructure.

On the technical side, bots can be categorized based on one or a combination of identifiers or signatures constructed from the request header content, request header order, origin response header content, user agent, cookie name and content, IPs, Geos, AS Num or AS Company Name, etc. This strategy involves putting one or multiple signatures into a category and then assigning an action to the category. With tens of thousands of different types of bots traversing the Internet, it is impossible to assign an action to each one individually. However, with proactive bot management it is possible to group together multiple bots that behave similarly and have a similar impact on the business and manage them as a group, rather than individually.

For example, instead of blocking all bots, IT may choose to **A)** allow all human traffic through; **B)** monitor bots that have legitimate use of the website, such as search engines, business partners, and vendors; **C)** serve alternate content to harmful bots like price scrapers and content aggregators; and **D)** redirect other bot traffic to an alternate origin where it can't impact user performance.

MANAGE, NOT MITIGATE

A more effective solution



MOTIVATION
The bot is here to get something

BLOCKING
Prevents the bot from getting what it came for

AWARENESS
Blocking also alerts bot operator

EVASION
Operator modifies the bot to evade detections/mitigations

WHACK-A-MOLE
The bot returns but is now better hidden from detection

A PROACTIVE SCENARIO: Manage bot traffic without alerting the operator

As mentioned earlier, bad bot operators can simply update their bot and try again every time they become aware that the bot has been blocked. Instead of blocking the bot and alerting the bot operator, a proactive bot management solution will offer several ways to either slow down the rate at which a bad bot can retrieve information or deceive the bot by feeding it different information than what it came for. Additionally, you can employ rate-based actions to minimize the impact of heavy traffic from good bots. In all cases, you can better manage the impact on your web infrastructure and maintain greater control over the information you choose to give to other parties on the Internet. You can determine if any, or all, of the following strategies for managing, not mitigating, bot activity is right for your business:

RATE-BASED ACTIONS TO DELAY OR SLOW THE RESPONSE

Websites can manage the impact on their origin of all types of bots by controlling how fast they allow them to scrape the site. This is useful for managing partner bots and other good bots that might otherwise cause performance degradation. Even for bad bots, sometimes the best course of action may be to give it the information it wants, but delay or slow the rate at which it can extract that information and minimize the impact on site performance.

SERVE ALTERNATIVE CONTENT

Organizations can control what content is returned to different types of bots for different purposes. For example, if a partner bot is scraping a site too aggressively, IT can serve an alternate page requesting the partner to stop scraping and instead utilize an API to obtain the information instead. On the other hand, to protect against price scraping by a competitor, an e-commerce site can serve the bot an alternative page that looks exactly like the real page, but with prices $10 higher. In this case, the operator thinks that the bot got the information it came for, but the e-commerce business is actually controlling the content provided.

SERVE ALTERNATIVE ORIGIN

Here, organizations can better manage the load on their origin from bot traffic. For example, businesses can set aside a number of high-performance servers just for legitimate users and a few other servers for bot categories determined by the business as well as bad bots detected in real-time.

SERVE CACHED CONTENT

This approach also minimizes load on the origin and returns information already cached without impacting site performance.

SIGNAL THE ORIGIN

In many cases, organizations may want to simply be alerted to bot traffic so that they can take action at the origin themselves. Here, a bot management solution should be able to insert identifying information into any web request identified as having been generated by a bot.

The bottom line is that blocking bots is no longer the best or only approach. Instead, taking a proactive bot management strategy provides more options for managing different types of bot traffic. What action on your part will make the bot (and the bot operator) think it got what it came for, but still minimize the impact on your infrastructure and business? Equally important, the bot management solution's reporting capability must provide sufficient granularity to verify that the correct action has been taken for each of the different bot types. You should be able to drill down into your bot traffic for analytics and sample log traffic that will indicate the bot's response to the action taken. Without this visibility, there would be no way to know for sure if the bot management solution deflected the bot's impact. In the end, even if you can only minimize the IT impact, taking some kind of action other than blocking is the still the best approach.

CHAPTER // 4

EVALUATING BOT MANAGEMENT SOLUTIONS

The following key capabilities should be part of any comprehensive bot management solution:

- *Identifies bots that are visiting the website.*
- *Helps companies quantify how much bot traffic is on the website.*
- *Provides enough visibility to help IT administrators analyze what individual bots have been doing on the site (scraping, adding comment spam, etc.).*
- *Reveals which parts of the site bots have been accessing and how frequently.*
- *Allows organizations to categorize different types of bots based on the impact on their business or IT infrastructure.*
- *Creates simple policies with different types of management actions that reflect and support business objectives and operational workflow.*
- *Provides enough visibility and granularity in its reporting that organizations can verify that the right actions were taken on different types of bots.*

WHY BOT MANAGEMENT?

FLEXIBILITY

Improve flexibility to manage bot traffic based on your unique needs to more effectively achieve your business goals.

VISIBILITY

Gain visibility into the characteristics and amount of bot traffic accessing your site.

PREVENTION

Maintain competitive advantage and generate more sales by preventing price and content scraping.

POLICY-BASED

Employ advanced strategies to better manage interactions with different types of bots based on business policy.

VALIDATION

Combat fraudulent activity by validating observed client behavior against legitimate user workflows.

PERFORMANCE

Improve web experience by reducing the impact of bots during regular business hours on the web infrastructure.

CONTROL

Retain control over customer relationships by preventing content aggregation that redirects customers to other sites.

REPORTING

Analyze/report ongoing bot traffic/ activity to measure the effectiveness of strategies and adapt to changes.

CHAPTER // 5

ADOPTING A PROACTIVE BOT MANAGEMENT PROCESS

As doing business on the Internet becomes more complex and sometimes dangerous, the time is right to gain deeper visibility into, and take greater control over, who actually accesses your websites and what actions they are taking – whether bot or human. While the actions of any user can cause concern, Internet bots in particular magnify the challenge due to their larger scale and the automated nature of their actions. Even small bots can generate a noticeable load on web infrastructure resources, while large bots can significantly degrade website performance and availability for legitimate users.

Although some commercial solutions available today can temporarily block any detected bots, you need a better, long-term bot management solution to reduce the impact of bots – and the stealthy actions of their operators – on both the web application infrastructure and the business.

Proactive bot management is an ongoing, iterative process that not only gives IT the visibility and control they need, but also translates into many business advantages. For example, organizations can ensure a consistent and positive user experience – and minimize lost sales and customer churn – by reducing or redirecting bot traffic during business hours. And, because bots can represent up to 35% of website traffic, IT can reduce or redirect bot traffic to consume fewer resources during peak times – resulting in reduced web infrastructure operating costs. In addition, the ability to more accurately identify bots through a bot management solution can guard against harmful bot activity — such as price list scraping by unscrupulous competitors – and help organizations maintain a competitive advantage and accurate data.

A REAL-WORLD SOLUTION: AKAMAI BOT MANAGER

To make these benefits available to organizations today, Akamai has introduced Bot Manager, an innovative bot management solution that complements the web security capabilities of a WAF and provides multiple techniques for bot visibility, detection, and management. Akamai's Bot Manager takes a turnkey approach to deliver the broadest set of bot detection methods, a massive cross-customer bot database based on significant portions of Internet traffic from major properties. The solution enables a flexible range of actions that can be applied to bot traffic to shape it, rather than just allowing or denying it. Akamai is uniquely positioned to bring this solution to the marketplace as up to 30% of all web traffic traverses its network on a daily basis, including the most important traffic to the largest and most frequently attacked sites in the world. We have deep visibility into how legitimate users use applications as well as the behavior of bad bots and how malicious bot attack vectors are constantly evolving and changing.

Learn more about Bot Manager at
www.akamai.com/bot-manager

Akamai

ABOUT AKAMAI

Akamai® is the leading provider of cloud services for delivering, optimizing, and securing online content and business applications. At the core of the Company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with first class reliability, security, visibility, and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

GOTBOTS?